CLAIMS

1. Method of automatic validation of a computer program able to access secure memory (MS) and non-secure memory (MNS), the program using at least one encryption function (DES) and at least one decryption function (DES-1), characterized in that it comprises a verification step (E340) which verifies that:

- any function adapted to read data from said secure memory (MS) and to produce data in said non-secure memory (MNS) is an encryption function; and

- any data produced by said decryption function is stored in said secure memory (MS).

2. Validation method according to claim 1, characterized in that said program also uses at least one non-cryptographic function, said non-cryptographic function being chosen from a logic function, a random number generation function and an integrity check function.

3. Validation method according to claim 2, characterized in that any data produced by said non-cryptographic function from data read in said secure memory (MS) is stored in said secure memory (MS).

4. Validation method according to any of claims 1 to 3, characterized in that, the computer program being in source code, the method comprises, before said verification step (E340), a step (E300) of compilation of said source code into binary script (EXE), said verification step (E340) being effected on the binary script (EXE) generated in this way.

5. Validation method according to any of claims 1 to 4, characterized in that said computer program is a sensitive data generation program.

6. Validation method according to any of claims 1 to 5, characterized in that said computer program is a sensitive data transformation program.

7. Validation method according to any of claims 1

to 6, characterized in that each function used by said computer program is associated with at least one operating mode that defines at least one rule governing access to said memories, said operating mode being stored in a verification table (TV) used during said verification step (E340).

8. Validation method according to claim 7, characterized in that it further comprises:

- a step (E310) of allocation of said secure memory (MS) and said non-secure memory (MNS);
- a step of loading into a working memory a verifier program for said binary script (EXE), said verifier program being adapted to implement said verification step (E340); and
- a step (E305) of loading said binary script (EXE) into said working memory.

9. Compiler characterized in that it is adapted to implement a validation method according to any of claims 1 to 7.

10. Method of executing a computer program adapted to access secure memory (MS) and non-secure memory (MNS), the program using at least one encryption function (DES) and at least one decryption function (DES-1), characterized in that a verification step (E340) conforming to any of claims 1 to 8 is executed before the execution (E420) of each function of said program.

11. Use of the execution method according to claim 10 to transform or generate sensitive data.

12. Use of the execution method according to claim 10 to customize microcircuit cards.

13. Integrated electronic circuit characterized in that it is adapted to implement a validation method according to any of claims 1 to 8 or an execution method according to claim 10.

14. Microcircuit card characterized in that it

comprises an integrated electronic circuit according to claim 13.

15. Computer system characterized in that it comprises an electronic integrated circuit according to claim 13.

16. Secure operating system adapted to implement a validation method according to any of claims 1 to 8.

17. Microcircuit card characterized in that it comprises an operating system according to claim 16.

18. Computer system characterized in that it comprises an operating system according to claim 16.

19. Device for validating a computer program adapted to access secure memory (MS) and non-secure memory (MNS), the program using at least one encryption function (DES) and at least one decryption function (DES-1), characterized in that it comprises a verifier program adapted to verify that:

- any function adapted to read data from said secure memory (MS) and to produce data in said non-secure memory (MNS) is an encryption function; and
- any data produced by said decryption function is stored in said secure memory (MS).

20. Validation device according to claim 19, characterized in that the verifier program is adapted to effect said verifications on the basis of a binary script (EXE) obtained by compilation of said computer program.

21. Computer system comprising a secure operating system characterized in that it comprises:

- means for compiling a computer program in binary script (EXE);
- means for loading said binary script (EXE) into a working memory;
- means for allocating secure memory (MS) and non-secure memory (MNS); and
- a validation device according to claim 19.